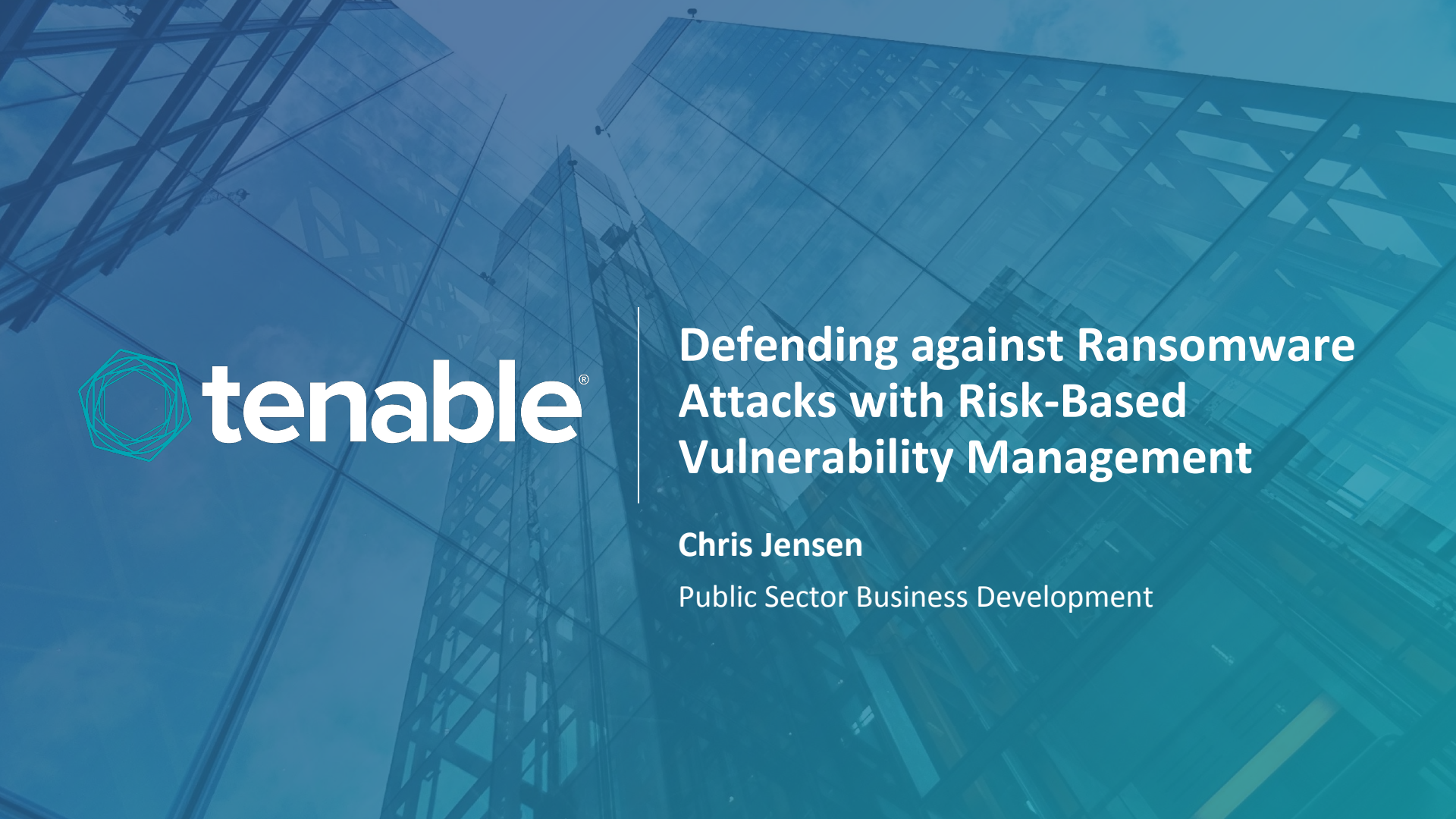


Defending against Ransomware Attacks with Risk-Based Vulnerability Management

Chris Jensen

Public Sector Business Development

Google

Ransomware

All | News | Images | Videos | Books | More | Settings | Tools

About 5,730,000 results (0.37 seconds)

ProPublica

The Ransomware Superhero of Normal, Illinois

Thanks to Michael Gillespie, an obscure programmer at a Nerds on Call repair store, hundreds of thousands of ransomware victims have ...

2 days ago

Las Cruces Sun-News

Ransomware hits Las Cruces school servers, prompts shutdown

This story was updated at 2:43 p.m.. LAS CRUCES - A ransomware attack prompted a shutdown of computers and internet servers across Las ...

18 hours ago

Insurance Journal

Ransomware Attacks Rise 37% in Q3, Targeting IT Vendors, Their Clients: Beazley

Ransomware attacks increased by 37% during the third quarter of 2019, compared to Q2, as cyber criminals target both IT vendors and their ...

23 hours ago

13WMAZ.com

Macon Water Authority online services hit with ransomware attack

MACON, Ga. — The Macon Water Authority says their servers are recovering after a ransomware attack that happened Sunday. According to a

SANS NewsBites

Annotated News Update from the Leade
Training, Certification and Research

October 29, 2019 Vol. 21, Num. 085

Top of The News

- Insurance Companies See Increasing Numbers of Ransomware Claims
- Johannesburg City Data Held for Ransom
- St. Louis Healthcare and Social Services Provider Struggling with Ransomware Attack

Cyber

SANS
Washin

SANS

tenable

PREVENTION VS. CURE

- Complete ransomware protection is multi-phased:
  - Preventing attacks
  - Backing up data to minimize damage from an attack
  - Building in resiliency to recover quickly from an attack

- This briefing focuses on prevention

tenable®

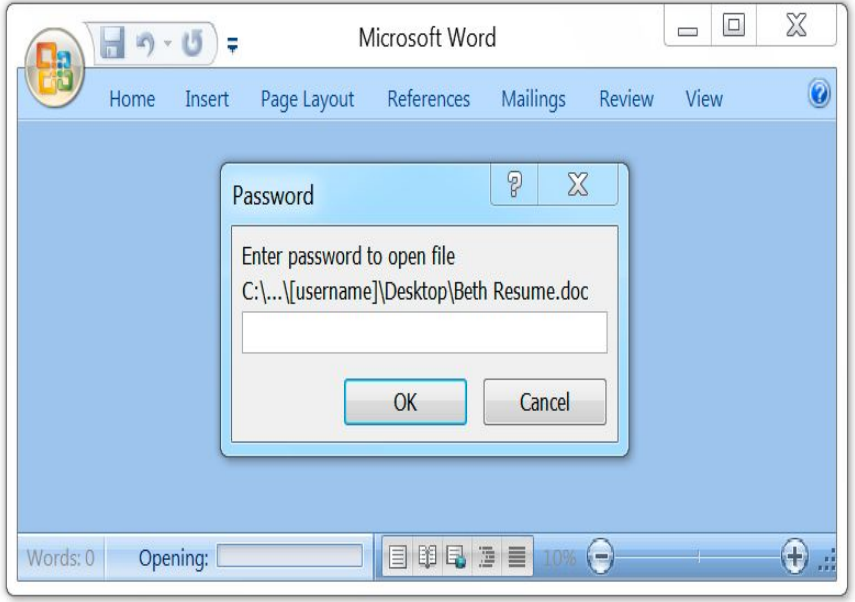
DEFENDING YOUR NETWORK “HOME”

- Hackers are not specifically targeting you; they are looking for easy targets
- Local governments are appealing targets in general – lots of valuable PII, but limited budgets and resources
- It’s a big neighborhood (over 75,000 local government entities in the US)
- Be the hard target; send hackers to a softer target down the street

tenable®

Ransomware Infection Techniques

Malicious Emails – Opening the Door



tenable

Bruteforce – Exploiting weak locks

Software Vulnerabilities

– Breaking In

DARKReading

9/26/19

Ransomware Hits Multiple, Older Vulnerabilities

Ransomware attacks are taking advantage of vulnerabilities that are older and less severe, a new report finds.

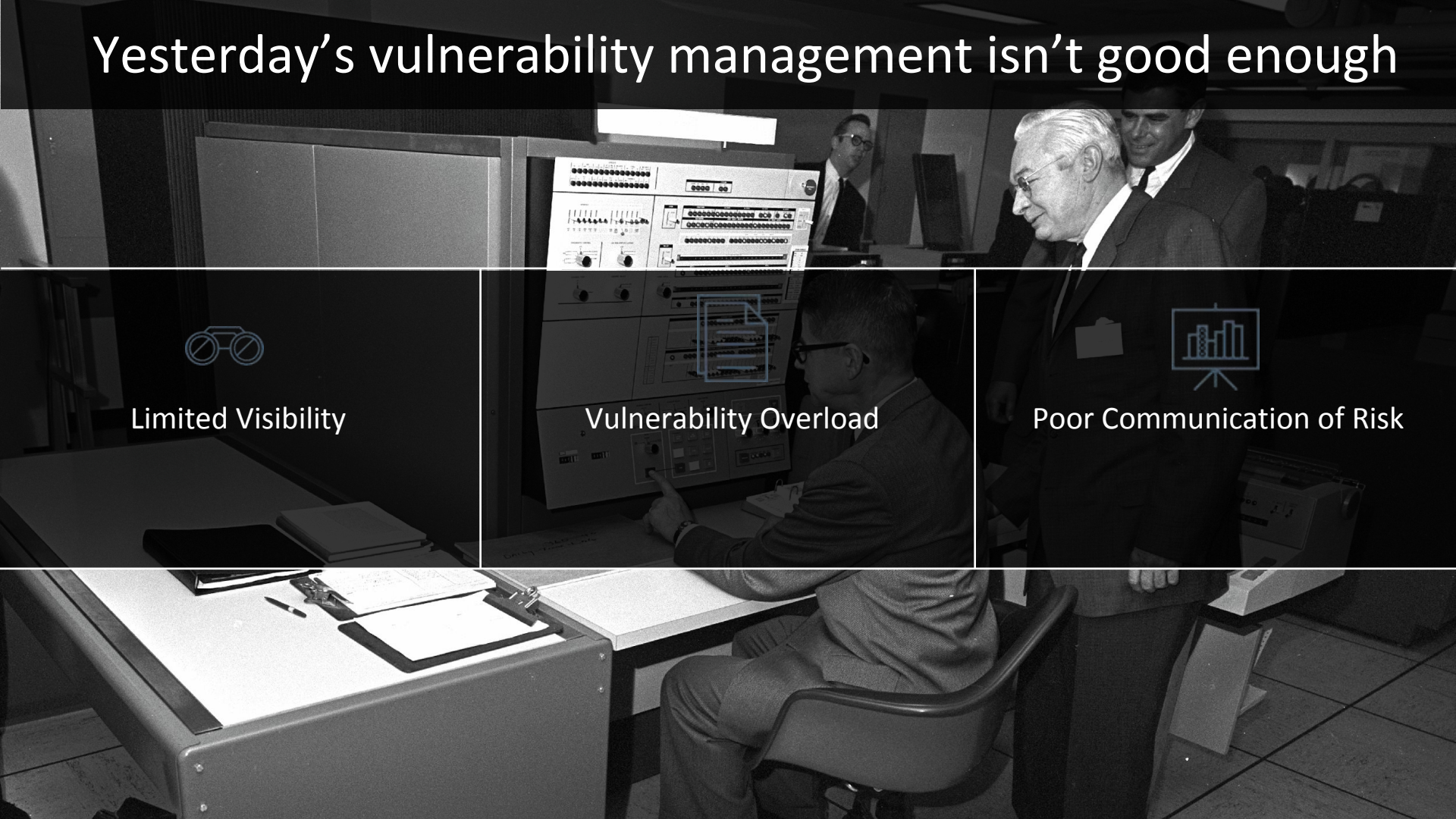
Ransomware attacks are taking advantage of vulnerabilities that might have gone unnoticed by security teams, with more than half of exploited vulnerabilities having a CVSS v2 score less than 8.

This 2019 report found that **35% of the vulnerabilities exploited in ransomware attacks were more than 3 years old**.

Source: https://www.darkreading.com/vulnerabilities---threats/ransomware-hits-multiple-older-vulnerabilities-/d/d-id/1335930

tenable

Yesterday’s vulnerability management isn’t good enough



Limited Visibility

Vulnerability Overload

Poor Communication of Risk

Upgrade to Risk-based Vulnerability Management

- See the full attack service
- Eliminate vulnerability overload
- Measure risk, not vulnerabilities

tenable

Risk-Based Vulnerability Management

Risk-Based Vulnerability Management (RBVM) is a process that uses machine learning analytics to correlate vulnerability severity, threat actor activity and asset criticality to identify and manage issues posing the greatest risk.

From **Vulnerability Management** to **Risk Based VM**

TRADITIONAL VULNERABILITY MANAGEMENT

People Powered

Focused on compliance

Adhoc & lightweight assessments

CVSS

Prioritization based on technical factors

Answers the questions:

- What assets do we have?
- Where are we exposed?

RISK BASED VULNERABILITY MANAGEMENT

Powered by Prediction

Focused on risk reduction

Continuous in-depth assessment of the converged attack surface

RBVM

Prioritization based on threats and business impact

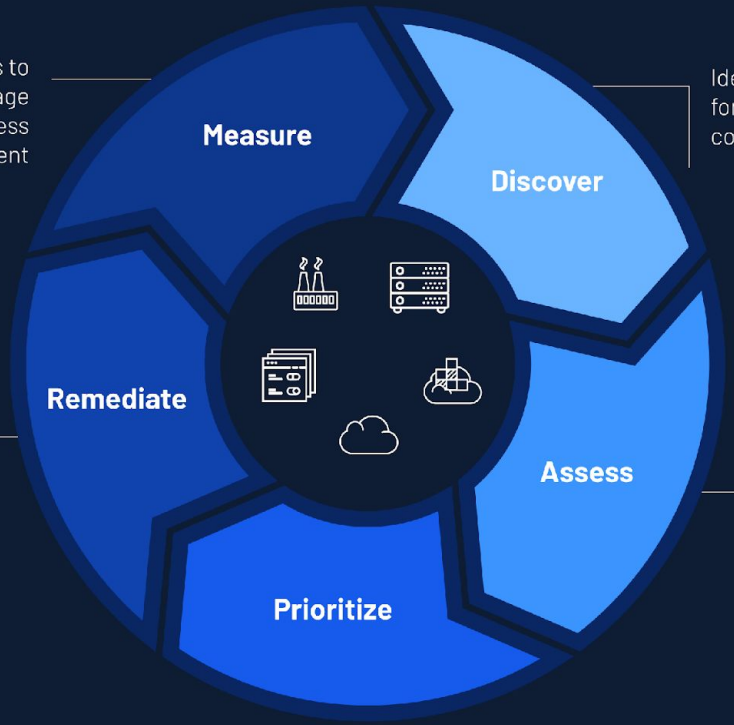
Answers the questions:

- Where should we prioritize based on risk?
- What is the impact if a vulnerability is exploited?
- What should we focus on first?

COMPARING LEGACY VM TO RBVM

VM		RBVM
Compliance Driven	→	**Risk Driven**
Infrastructure/IT Focus	→	**Expansion to Apps & Modern Assets**
Static, Point in Time Visibility	→	**Dynamic, Continuous Visibility**
Policies & Audit Support	→	**Prioritization & Strategic Decision Support**
Reactive	→	**Proactive**
Vulnerability Data Only	→	**Vuln Data Correlated w/ Threat Intelligence & Asset Criticality**

The Cyber Exposure Lifecycle for Risk Based VM



Measure key metrics to identify gaps in coverage and areas for process improvement

Identify and map every asset for visibility across any computing environment

Understand the state of all assets, including vulnerabilities, misconfigurations and other health indicators

Leveraging threat intelligence and business context to focus on vulnerabilities that are likely to be exploited

Ensure mitigation methods are implemented and patches deployed accurately

tenable

Prioritize Vulnerabilities and Assets

tenable

16500+

VULNERABILITIES DISCLOSED IN 2018

59%

Of vulnerabilities disclosed in 2018 were rated critical or high.

Over 9,500+ Vulnerabilities

15%

Of vulnerabilities disclosed in 2018 were CVSS 9+

2,500 Vulnerabilities

7%

Of vulnerabilities disclosed had publicly available exploits

Over 1,100 Vulnerabilities

tenable

VPR

VULNERABILITY PRIORITY RATING

Leverages supervised machine learning algorithms to calculate the priority of a vulnerability based on the real threat posed.

Key Drivers include


Threat Recency

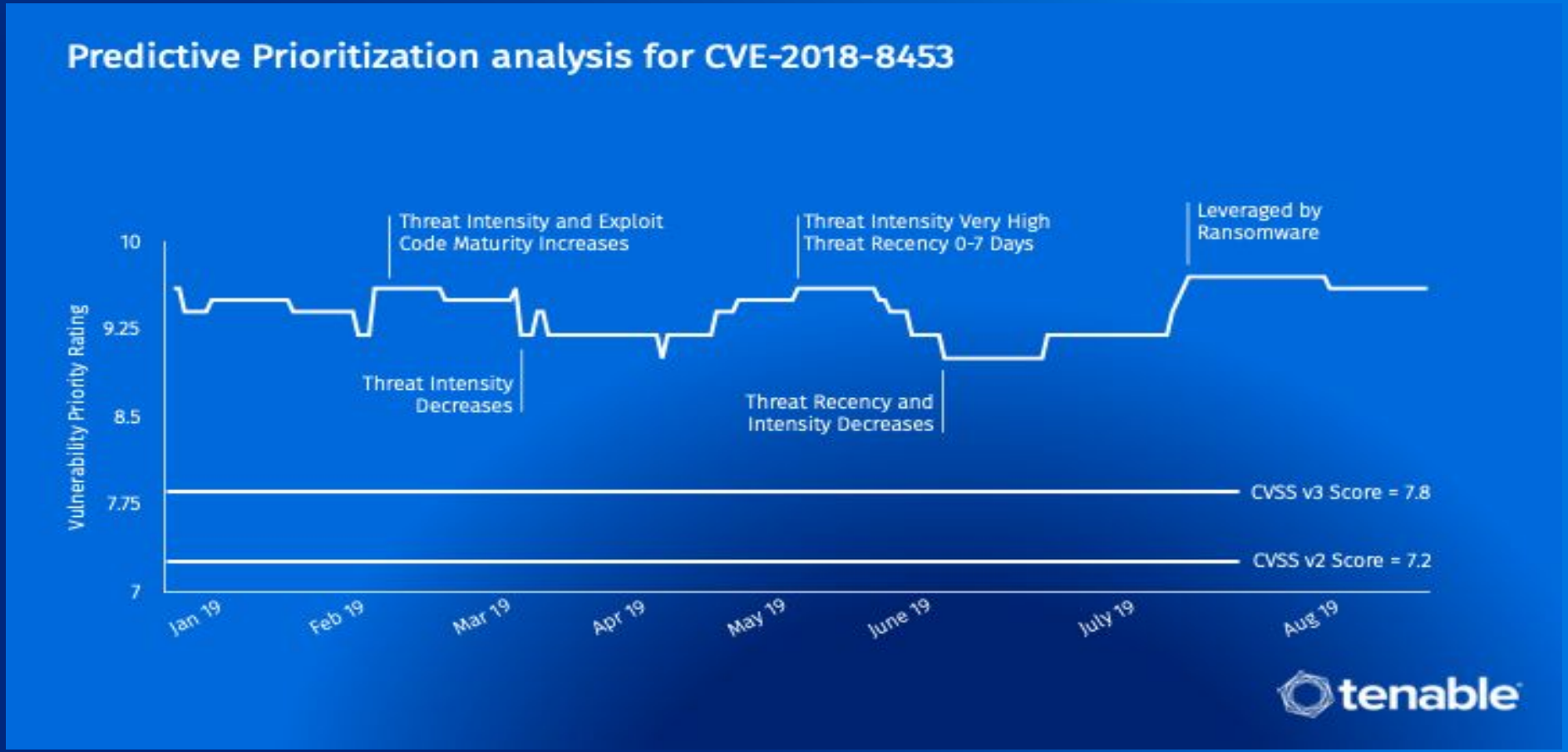

Threat Intensity


Exploitability


Vulnerability Age


Threat Sources

Elevation of privilege vulnerability in Windows
Used in Texas (+ other) 2019 ransomware attacks



ACR

ASSET CRITICALITY RATING

Leverages algorithms to calculate the criticality of an asset to focus prioritization efforts.
Key drivers include


Business Purpose


Device Type


Connectivity


Capabilities


Location


3rd Party Data

FOCUS FIRST ON WHAT MATTERS MOST

VPR

VULNERABILITY PRIORITY RATING

Leverage machine learning and **threat** intelligence to prioritize vulnerabilities based on **likelihood** of exploitation

+

ACR

ASSET CRITICALITY RATING

Prioritize assets based on the indicators of business value and **impact**

=

CES

CYBER EXPOSURE SCORE

Objectively measure the Cyber Risk of an asset, business unit or whole organization

tenable

FORRESTER®

"Tenable executes on its vision to build the **single-source-of-truth platform for VRM.** Part of Tenable's strong strategy relies on **translating data to provide business insight** to provide prioritization."

Thank you

tenable